UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/741,680	12/15/2000	Vipin Samar	OR00-14001	6541

51067	7590	12/05/2006

ORACLE INTERNATIONAL CORPORATION
c/o PARK, VAUGHAN & FLEMING LLP
2820 FIFTH STREET
DAVIS, CA 95618-7759

EXAMINER
NGUYEN, CAM LINH T

ART UNIT	PAPER NUMBER
2161	

DATE MAILED: 12/05/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on *27 September 2006*.

2a) ☐ This action is **FINAL**.   2b) ☒ This action is non-final.

3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) *49-66* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) ☐ Claim(s) _____ is/are allowed.

6) ☒ Claim(s) *49-66* is/are rejected.

7) ☐ Claim(s) _____ is/are objected to.

8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.

10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a) ☐ All   b) ☐ Some * c) ☐ None of:

      1. ☐ Certified copies of the priority documents have been received.

      2. ☐ Certified copies of the priority documents have been received in Application No. _____.

      3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date _____.

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1.   A request for continued examination under 37 CFR 1.114, including the fee set forth in

37 CFR 1.17(e), was filed in this application after final rejection. Since this application is

eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e)

has been timely paid, the finality of the previous Office action has been withdrawn pursuant to

37 CFR 1.114. Applicant's submission filed on 9/27/2006 has been entered.

2.   Applicant's amendments to claims 49-66 are acknowledged. Consequently, claims 49 –

66 are currently pending.

Claim Rejections - 35 USC § 112

3.   The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4.   Claims 49 – 66 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite

for failing to particularly point out and distinctly claim the subject matter which applicant

regards as the invention.

5.   Claims 49, 55, 61 recite the limitation "security officers" in the preamble of the claims.

However, there is another "security officer who is the only database administrator empowered to

perform administrative functions…" in the last limitation of each independent claim. The

Examiner is not sure if this "security officer who is the only database administrator" is different

from the "security officers" that were referenced in the preamble.

Claim Rejections - 35 USC § 103

1.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in
> section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are
> such that the subject matter as a whole would have been obvious at the time the invention was made to a person
> having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the
> manner in which the invention was made.

2.   Claims 49 – 50, 54 – 56, 60 – 62, 66 are rejected under 35 U.S.C. 103(a) as being

unpatentable over D. Richard Kuhn (U.S. 6,023,765) in view of Sweet et al (U.S. 2002/0031230

A1).

♦ As per claims 49, 55, 61

Kuhn discloses a method/a computer-readable storage medium (corresponds to MLS system, col.

4, lines 25 - 30) and an apparatus for managing a database system, comprising:

-   "Receiving a command to perform an administrator function involving a user within the

    database system" (See Fig. 3, col.7, lines 65 - 66). Any type of users can make the

    command in the privileged classes (Fig. 1, element 10). "Involving a user within the

    database system" corresponds to a object or documents or employ resources (col. 4, lines

    53 – 56).

-   "Determining if the user is a sensitive user who is empowered to access sensitive data in

    the database system". In this case, the Examiner interpret the phrase "the user is a

    sensitive user who is empowered to access sensitive data in the database system" as a

    "document or employ resource" that are protected in the system. The object is attached

    label such as "CONFIDENTIAL, SECRET, TOP SECRET" (col.6, lines 53 – 55). Kuhn

    teaches that in order to access to the object, it must determine the sensitivity level of the

    information (Col. 10, lines 10 – 12).

- " If the user is not a sensitive user, and if the command is received from a normal database administrator for the database system, allowing the administrative function to proceed" (See col. 7, lines 18 – 24, 65 – col. 8, lines 4). Kuhn teaches that the system would only allow the use access to the object when the security levels equal or less than his/her own clearance level using the mapping. Therefore, if the document is not sensitive (not a sensitive user) such as having labeled "confidence", and the user is having a "confidence" level (normal administrator), then the systems will "allowing the administrative function to proceed".

- " If the user is a sensitive user, and if the command is received from a normal database administrator, preventing the normal database administrator from performing the administrative function involving the sensitive user" (See col. 7, lines 18 – 24, 65 – col. 8, lines 4). As discussed above, Kuhn teaches that the system would only allow the use access to the object when the security levels equal or less than his/her own clearance level using the mapping. Therefore, if the document is sensitive (a sensitive user) such as having labeled "top secret", and the user is having a "confidence" level (normal administrator), then the systems will "disable the administrative function to proceed".

- " If the user is a sensitive user, and if the command is received from a security officer who is the only database administrator empowered to perform administrative functions for sensitive users, allowing the administrative function to proceed". Again, by applying the same test above, the system would allow the security officer to perform the administrative function since the security officer is the highest level in the database system.

- " A command receiving mechanism configured to receive a command" corresponds to

   the external system 24 (See Fig. 2, element 24).

Kuhn does not clearly teach that the database system has a plurality of administrators, and at

least one of the pluralities of administrators is a security officer who can perform administrative

functions on sensitive objects. Kuhn is silent on teaching that the database system includes

normal database administrators, and security officers.

However, Sweet, on the other hand, discloses a security system that comprises:

- " Plurality of administrators" page 7, paragraph 0090.

- "The sensitive object" See page 6, paragraph 0081.

- " Wherein at least one of the plurality of administrators is a security officer who can

   perform administrative functions on sensitive objects" See page 7, paragraph 0090.

- " Wherein an administrator in the plurality of administrators who is not a security officer

   cannot become a sensitive user and thereby obtain access to sensitive objects indirectly"

   See page 7, paragraph 0091. Wherein, "an administrator in the plurality of administrators

   who is not a security officer" can be a normal administrator in domain 125, who is

   responsible for the configuration and management only.

- "If the object is not a sensitive object, and if the command is received from an

   administrator who is not a security officer; allowing the administrative function to

   proceed" page 7, paragraph 0090 – 0091, 0152.

- "If the object is a sensitive object, and if the command is received from an administrator

   who is not a security officer, disallowing the administrative function" page 7, paragraph

   0090 – 0091, 0165.

As discussed above, the Sweet discloses a hierarchical administrative group according to different levels of administrative tasks (see page 3 paragraph 0035 of Sweet), and Kuhn teaches that depending on user privileges, the system will allow the user to access to the object (See col. 7, lines 18 – 24, 65 – col. 8, lines 4 of Kuhn).

It would have been obvious to one with ordinary skill in the art at the time the invention was made to apply the teaching of Sweet into the system of Kuhn because both invention were available and the teaching of Sweet provides secure electronic access to the system using the security officer and adminstrators; the combination would protect the database more secure by using different administrator levels so that an administrator in the plurality of administrators who is not a security officer (using administrator group in Sweet) cannot perform administrative functions on sensitive object (using Kuhn invention).

♦ As per claims 50, 56, 62, Kuhn and Sweet disclose:

- "A request to perform an operation" corresponds to "a command to perform an administrative function" See Fig. 3, col.7, lines 65 – 66 of Kuhn.

- " If the data item is a sensitive data item containing sensitive information and if the request is received from a sensitive user who is empowered to access sensitive data, allowing the operation to proceed if the sensitive user has access rights to the sensitive data item" The Examiner in this case will interpret the "data item" as "document" in Kuhn reference. Again, by applying the same test above, the system would allow the sensitive user who is empowered to access sensitive data to perform the administrative function since the sensitive user is the highest level in the database system (See col. 7, lines 18 – 24, 65 – col. 8, lines 4 of Kuhn).

- " If the data item is a sensitive data item and the request is received from a user who is not a sensitive user, disallowing the operation" (See col. 7, lines 18 – 24, 65 – col. 8, lines 4). As discussed above, Kuhn teaches that the system would only allow the use access to the object when the security levels equal or less than his/her own clearance level using the mapping. Therefore, if the document is sensitive (a sensitive data) such as having labeled "top secret", and the user is having a "confidence" level (not a sensitive user), then the systems will "disable the administrative function to proceed".

♦ As per claims 54, 60, 66, Kuhn and Sweet disclose:

- " Wherein if the user is not a sensitive user, and if the command to perform the administrative function is received from a security officer, the method further comprises allowing the security officer to perform the administrative function on the user" See col. 7, lines 18 – 24, 65 – col. 8, lines 4 of Kuhn.

3.   Claims 51 – 53, 57 – 59, 63 – 66 are rejected under 35 U.S.C. 103(a) as being unpatentable over D. Richard Kuhn (U.S. 6,023,765) in view of Sweet et al (U.S. 2002/0031230 A1) as applied to claims 49 - 50 above, and further in view of Minear et al (U.S. 5,983,350).

♦ As per claim 51 - 53, 57 – 59, 63 – 66, Kuhn and Sweet disclose:

The combination of Kuhn and Sweet fail to disclose:

- " Wherein if the data item is a sensitive data item, if the operation is allowed to proceed, and if the operation involves retrieval of the data item, the method further comprises decrypting the data item using an encryption key after the data item is retrieved".

However, this is a well-known technique in the art to protect the data when transferring in the

network. Minear provided an example of it. Minear teaches a method for securely transferring

information in the network (col. 1, lines 8 – 11, Minear) comprising the decrypting/encrypting

data (col. 2, lines 52 – 64, Minear). Minear also teaches that the encryption key is stored in a

table (col. 7, lines 29 – 35, Minear).

It would have been obvious to one with ordinary skill in the art at the time the invention was

made to apply the teaching of Minear into the combination of Kuhn/Sweet because the

combination would protect the data more secure and prevent the unauthorized user to access the

data.

Response to Arguments

4.   Applicant's arguments filed 5/12/2006 have been fully considered but they are not

persuasive.

   Applicant argues that Kuhn or Sweet do not teach a database system includes sensitive

users, normal administrators, and security officers (page 10 of the Remark). The Examiner

respectfully disagrees.

   First of all, the claims language stated, " a security officer who is the only database

administrator empowered to perform administrative function involving sensitive user". Kuhn and

Sweet teach this limitation. Therefore, the security officer or "special administrator" can either

perform administrator function on either sensitive user or normal user.

Secondly, the Examiner did not user the Kuhn reference to teach about the security officer or the

"special administrator". Instead, the Examiner uses the Sweet reference to disclose this. In Sweet

reference, the security officer is the highest level that can create and maintain the information in

the domain (paragraph 0090). The applicant also admitted that the Sweet reference manages the

security profile (page 9 of the remark). Therefore, the Kuhn and Sweet references clearly

disclose a special administrator who manages only sensitive user.

As discussed above, Sweet teaches that the security officer is the highest level that can

create and maintain the information in the domain (paragraph 0090). The applicant also admitted

that the Sweet reference manages the security profile (page 9 of the previous remark). Therefore,

the security office in this embodiment is the only database administrator empowered to perform

administrative functions on sensitive users. Applicant referrers to paragraph 0247 stated that

there is multiple administrators can maintain the security user (page 9 of the previous Remark).

However, this is just a general situation. In particular situation, the security officer is the highest

person can create or grant the authority to the administrators (paragraph 0090). Depend on the

size of the domain, the security officer can grant only one database administrator to manage the

user profile or sensitive user data. Therefore, in this situation, the security officer is the only

database administrator empowered to perform administrative functions on sensitive users as

claimed in the claims invention.

Conclusion

5.   Any inquiry concerning this communication or earlier communications from the

examiner should be directed to CamLinh Nguyen whose telephone number is (571) 272-4024.

The examiner can normally be reached on Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, GAFFIN JEFFREY A can be reached on (571) 272-4146146. The fax phone number

for the organization where this application or proceeding is assigned is 571 – 273- 8300.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Nguyen, Cam Linh
Art Unit 2161
LN